

3. Complementi

Qualche idea sulla struttura di gruppo

Abbiamo visto nel testo (in particolare nei paragrafi 8 e 9) come sia proprio la corrispondenza fra la moltiplicazione di numeri e l'addizione dei logaritmi dei numeri stessi ad aver suggerito di svolgere i calcoli con i logaritmi. Si sostituisce in tal modo ad un'operazione spesso complicata come la moltiplicazione l'operazione più semplice di addizione.

In questo complemento vogliamo studiare più a fondo questa corrispondenza fra numeri e logaritmi.

Sappiamo che se a e b sono due numeri reali positivi, si ha

$$\log a = m, \quad \log b = n,$$

dove m e n sono numeri reali.

Valgono le seguenti proprietà:

$$1) \log(a \cdot b) = m + n$$

$$2) \log 1 = 0$$

$$3) \log\left(\frac{1}{a}\right) = -m.$$

La dimostrazione di queste proprietà non è difficile, ma molto spesso non è facile valersi delle proprietà con disinvoltura quando si svolgono i calcoli. La difficoltà è dovuta al fatto che nel passaggio dalla moltiplicazione all'addizione occorre tener presenti le "nuove" proprietà dei logaritmi assieme alle "vecchie" proprietà della moltiplicazione e dell'addizione. Vogliamo ora vedere come "nuove" e "vecchie" proprietà possono fondersi quando vengono considerate da un diverso punto di vista.

Cominciamo col riflettere sulle proprietà più significative dell'addizione e della moltiplicazione; si ha:

addizione	moltiplicazione
I) commutativa: $m+n=n+m$	I') commutativa: $a \cdot b = b \cdot a$
II) associativa: $m+(n+p)=(m+n)+p$	II') associativa: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
III) esiste un numero 0 tale che $m+0=m$	III') esiste un numero 1 tale che $a \cdot 1 = a$

Si nota subito una stretta analogia fra le proprietà I e II dell'addizione e le corrispondenti proprietà I' e II' della moltiplicazione. Si è poi condotti ad "unificare" anche le proprietà III e III', e ciò in base alla seguente osservazione: la III afferma che, se si aggiunge 0 ad un qualunque numero m , il numero resta inalterato, cioè 0 è l'elemento neutro nell'addizione; la III' afferma che, se si moltiplica per 1 un

qualunque numero a , il numero resta inalterato, cioè 1 è l'elemento neutro nella moltiplicazione. Si trovano poi queste altre proprietà:

IV) si può ottenere 0 addizionando un numero (m) col suo opposto ($-m$), ossia $m + (-m) = 0$;

IV') si può ottenere 1 moltiplicando un numero (a) per il suo inverso $\left(\frac{1}{a}\right)$, cioè $a \cdot \frac{1}{a} = 1$.

È importante osservare che queste proprietà che sembrano tanto evidenti non sono sempre valide. Ecco qualche esempio:

- se si esegue la moltiplicazione fra numeri interi, non esiste, per ogni intero, il suo inverso; per esempio, non esiste l'inverso di 3 perché $\frac{1}{3}$ non appartiene all'insieme degli interi;
- se si esegue la moltiplicazione fra numeri pari, non esiste l'elemento neutro perché 1 non appartiene all'insieme dei pari;
- se si esegue l'addizione di due numeri dispari, si ottiene un numero pari; perciò, se ci si limita all'insieme dei dispari, non è possibile eseguire l'addizione, perché, in questo insieme, non si trova il risultato dell'addizione.

Si capisce quindi che per esaminare in modo chiaro le proprietà che abbiamo elencato si deve precisare:

- l'insieme dei numeri su cui si opera,
- l'operazione che associa ad ogni coppia di numeri dell'insieme un terzo numero (il risultato dell'operazione).

Torniamo ora alla corrispondenza fra numeri e logaritmi.

Da un lato, si opera con la moltiplicazione sull'insieme R^+ dei reali positivi (in cui si scelgono i numeri a, b, \dots), dall'altro si opera con l'addizione sull'insieme R dei reali (in cui si trovano i numeri $m = \log a, n = \log b, \dots$). In questo caso valgono le seguenti 4 proprietà:

- R con l'addizione
- I) commutativa: $m+n=n+m$
 - II) associativa: $m+(n+p)=(m+n)+p$
 - III) esiste 0 tale che $m+0=m$
 - IV) esiste l'opposto ($-m$) di ogni m , tale che $m+(-m)=0$

- R^+ con la moltiplicazione
- I') commutativa: $a \cdot b = b \cdot a$
 - II') associativa: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
 - III') esiste 1 tale che $a \cdot 1 = a$
 - IV') esiste l'inverso $\left(\frac{1}{a}\right)$ di ogni a , tale che $a \cdot \frac{1}{a} = 1$.

L'analogia fra le due situazioni è, ora, meglio precisata: l'insieme R rispetto all'addizione e l'insieme R^+ rispetto alla moltiplicazione hanno la stessa struttura. A questa struttura caratterizzata dalle 4 proprietà sopra elencate si dà il nome di *gruppo*; si dice cioè che l'insieme R forma gruppo rispetto all'addizione e che l'insieme R^+ forma gruppo rispetto alla moltiplicazione.

Per quanto si è visto, questi due gruppi possono essere collegati fra loro associando ad ogni numero reale positivo il suo logaritmo (per esempio a base 10); la situazione è visualizzata nello schema seguente:

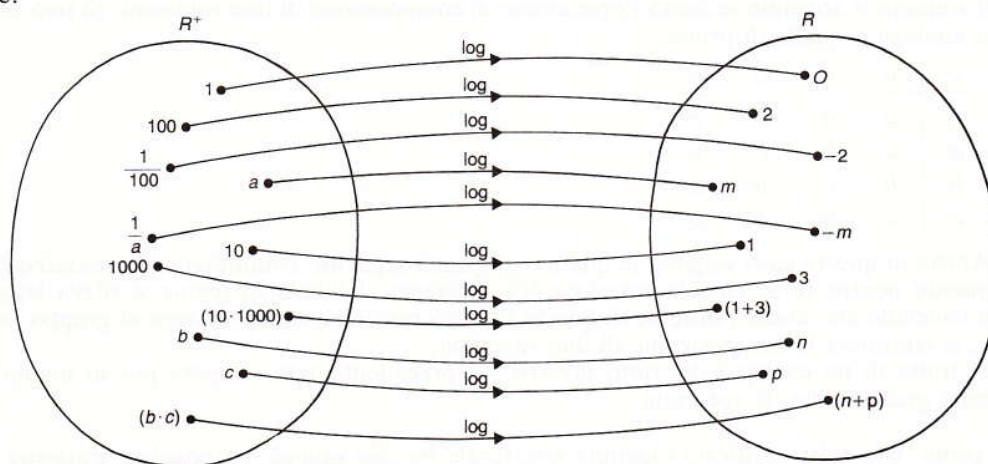


Fig. 13

La figura mostra come il logaritmo stabilisca una corrispondenza biunivoca fra l'insieme R^+ e l'insieme R : ad ogni numero reale positivo corrisponde il suo logaritmo, e viceversa. Tale corrispondenza

biunivoca, che "conserva le operazioni", dà un esempio di *isomorfismo*: l'insieme dei numeri reali positivi e l'insieme dei logaritmi di tali numeri sono gruppi isomorfi, cioè di "ugual forma", di uguale struttura.

Da quanto si è visto, la struttura di gruppo sembra trovarsi solo quando si considerano operazioni, come l'addizione e la moltiplicazione, fra numeri reali. Faremo ora vedere che, invece, si può trovare questa struttura negli "ambienti" più diversi. Ecco qualche esempio:

1) risolviamo l'equazione

$$x^4=1;$$

si hanno le 4 soluzioni:

$$1 \quad -1 \quad i \quad -i.$$

Questi quattro numeri, chiamati radici quarte dell'unità, sono legati fra loro dalle seguenti relazioni:

$$i^2=-1, \quad i^3=i^2 \cdot i=-1, \quad i^4=i^2 \cdot i^2=1.$$

Se si opera con la moltiplicazione nell'insieme delle quattro radici dell'unità, si ottiene sempre un risultato che appartiene allo stesso insieme; nella tabella seguente, da leggersi come una tavola pitagorica, sono indicati tutti i prodotti:

•	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

È facile verificare che valgono le quattro proprietà seguenti: commutativa, associativa, esistenza dell'elemento neutro (è il numero 1), esistenza dell'inverso (l'inverso di i è $-i$, e viceversa, l'inverso di 1 è 1, l'inverso di -1 è -1). Questo insieme ha perciò, rispetto alla moltiplicazione, la struttura di gruppo.

Si nota tuttavia una differenza rispetto ai due gruppi esaminati prima: ora l'insieme non è infinito, come quello dei reali, ma è *finito*, dato che si compone solo di quattro elementi.

2) consideriamo le seguenti quattro rotazioni del piano attorno al punto O :

u : rotazione di 0°

a : rotazione di 90° in senso antiorario

b : » » 180° » » »

c : » » 270° » » »

Proviamo a comporre due di queste rotazioni: ruotando prima di 90° e poi di 180° si ottiene una rotazione di 270° , ... Scriviamo brevemente questi risultati al modo seguente

$$a \circ b = c,$$

dove con il simbolo \circ abbiamo indicato l'operazione di composizione di due rotazioni. Si può compilare una tabella analoga a quella di prima:

\circ	u	a	b	c
u	u	a	b	c
a	a	b	c	u
b	b	c	u	a
c	c	u	a	b

Anche in questo caso valgono le quattro proprietà seguenti: commutativa, associativa, esistenza dell'elemento neutro (è u , cioè la rotazione 0°), esistenza dell'inverso (come si rileva leggendo la tabella). Si conclude che anche l'insieme di queste quattro rotazioni ha la struttura di gruppo, se, come operazione, si considera la composizione di due rotazioni.

Si tratta di un esempio del tutto diverso dai precedenti: non si opera più su numeri ma su trasformazioni geometriche, le rotazioni.

Si capisce come, una volta verificata l'identità strutturale fra due gruppi, sia possibile trasferire tutte le proprietà, che sono state scoperte per un gruppo, a un altro gruppo ad esso isomorfo; la ricerca viene, in tal modo, ridotta a un solo caso. È proprio questa possibilità di limitarsi all'analisi di un solo caso per illuminare lo studio di strutture uguali, anche se queste riguardano enti ed operazioni del tutto diverse, che costituisce la grande scoperta dell'*algebra astratta*, uno dei rami più fecondi della matematica d'oggi.